

User Guide

FORTANIX DATA SECURITY MANAGER - AZURE MANAGED HSM

VERSION 2.0

TABLE OF CONTENTS

1.0 INTRODUCTION 3

1.1 Overview3

1.2 Types of Azure BYOK flows.....3

2.0 DEFINITIONS..... 4

3.0 FORTANIX DATA SECURITY MANAGER AZURE MANAGED HSM GROUP WORKFLOW 6

3.1 Azure App Configuration.....6

3.2 Create and Configure Azure Key Vaults11

3.3 Prerequisites.....11

3.4 Configure the Azure Managed HSM12

 3.4.1 Create Azure KMS Group.....12

3.5 Test Connection14

3.6 Select Azure Managed HSM Instance14

3.7 Add Certificate.....14

3.8 The HSM/KMS Tab15

3.9 Sync Keys15

3.10 Not Connected Scenario16

3.11 Groups Table View16

3.12 User View16

4.0 FORTANIX DATA SECURITY MANAGER AZURE MANAGED HSM SECURITY OBJECTS 17

4.1 Create a Key in Azure Managed HSM Group – Generate (Managed HSM Pool).....17

 4.1.1 Generate a Key.....17

 4.1.2 Bring You Own key – Import Key.....19

 4.1.3 Bring Your Own Key – copy Key to Azure Key Vault.....20

4.2 Attributes/Tags Tab22

- 4.3 Azure Key Details22
- 4.4 Security Objects Table View22
- 4.5 Deactivate a Key in Azure Group.....22
- 4.6 Soft Delete a Key in Azure Managed HSM.....22
- 4.7 Delete a Key in Azure Group.....23

- 5.0 ROTATE A KEY IN AZURE GROUP 24
- 5.1 Rotating Azure Native Key* With Another Native Key24
- 5.2 Rotating Keys in Fortanix Data Security Manager Source Group24
- 5.3 Rotate Azure native key to Fortanix Data Security Manager Owned Key25

- 6.0 DOCUMENT INFORMATION 26
- 6.1 Document Location.....26
- 6.2 Document Updates26
- 6.3 Revision History.....26

1.0 INTRODUCTION

Welcome to the Fortanix Data Security Manager (DSM) Azure Key Vault (AKV) Managed Hardware Security Module (HSM) Key Management Service (KMS) User Guide. This document describes how to add a new Azure AKV Managed HSM to Fortanix DSM. It contains the information related to:

- Creating a AKV Managed HSM backed group in Fortanix DSM
- Configuring the AKV Managed HSM Connection in Fortanix DSM
- Testing the AKV Managed HSM Connection
- Syncing the AKV Managed HSM keys in Fortanix DSM

1.1 OVERVIEW

The Fortanix solution for AKV Managed HSM KMS offers complete Bring Your Own Key (BYOK) and lifecycle management for management and automation of Azure Managed HSM keys and allows users to manage all keys centrally and securely.

1.2 TYPES OF AZURE BYOK FLOWS

- a. Fortanix DSM key BYOK into Standard Tier Azure Key Vault (Software-protected: FIPS 140-2 Level 1 compliance)
- b. Fortanix DSM Key BYOK into Premium Tier Azure Key Vault (HSM-protected: FIPS 140-2 Level 2 compliance)
- c. Fortanix DSM key BYOK from Fortanix DSM as HSM into Azure Key Vault HSM using custom Key wrapping inside Fortanix DSM
- d. Fortanix BYOK into Azure Managed HSM (HSM-protected: Azure FIPS 140-2 Level 3 compliance).

2.0 DEFINITIONS

- **Fortanix Data Security Manager -**

Fortanix DSM is the cloud solution secured with Intel® SGX. With Fortanix DSM, you can securely generate, store, and use cryptographic keys and certificates, as well as secrets, such as passwords, API keys, tokens, or any blob of data.

- **Accounts -**

A Fortanix DSM account is the top-level container for security objects managed by the Fortanix DSM. An account is generally associated with an organization, rather than an individual. Security objects, groups, and applications belong to exactly one account. Different accounts are fully isolated from each other. See [support](#) for more information.

- **Users -**

Users are associated with an email address. A user can be a member of one or more accounts. Depending on permissions, users can:

- Perform management operations like adding or modifying users or groups
- Create security objects
- Change properties of security objects
- Review logs of Fortanix DSM activity



Users cannot perform cryptographic operations. Only applications can perform cryptographic operations.

- **Groups -**

A group is a collection of security objects created by and accessible by users and applications which belong to the group. The user who creates a group automatically gets assigned the role of the group administrator. You can add more users to the group in the role of administrators or auditors. You can also add applications to the group to enable the applications to create and use security objects in that group. See [support](#) for more information.

Access policies are set at the group level, so all security objects in a group share the same access policy. Any number of users and/or applications can be assigned to a group. *Some examples of usage of groups are given in the [Authorization](#) section.*

Quorum policies can also be set at group level. A Quorum policy mandates that all security sensitive operations in that group would require a quorum approval. Such operations include using a key for cryptographic operations or deleting or updating a group. *See [Quorum Policy](#) for more information.*

- **Applications -**

An application can use Fortanix DSM to generate, store, and use security objects, such as cryptographic keys, certificates, or an arbitrary secret. Applications can authenticate to Fortanix DSM using an API key (a secret token) or a TLS client certificate. An application can interact with Fortanix DSM using the RfEST APIs or using the PKCS#11, JCE, or CNG providers. *See [support](#) for more information.*

- **Fortanix Data Security Manager Security Objects -**

A security object is any datum stored in Fortanix DSM (for example a key, a certificate, a password, or other security objects). Each security object is assigned to exactly one group. users and applications assigned to the group have permission to see the security object and to perform operations on it. *See [support](#) for more information.*

3.0 FORTANIX DATA SECURITY MANAGER AZURE MANAGED HSM GROUP WORKFLOW

3.1 AZURE APP CONFIGURATION

Register Fortanix DSM as an app in Azure and get the app’s Active Directory (AD) credentials as explained below.

1. Log in to <https://portal.azure.com/>.
2. Register an application.

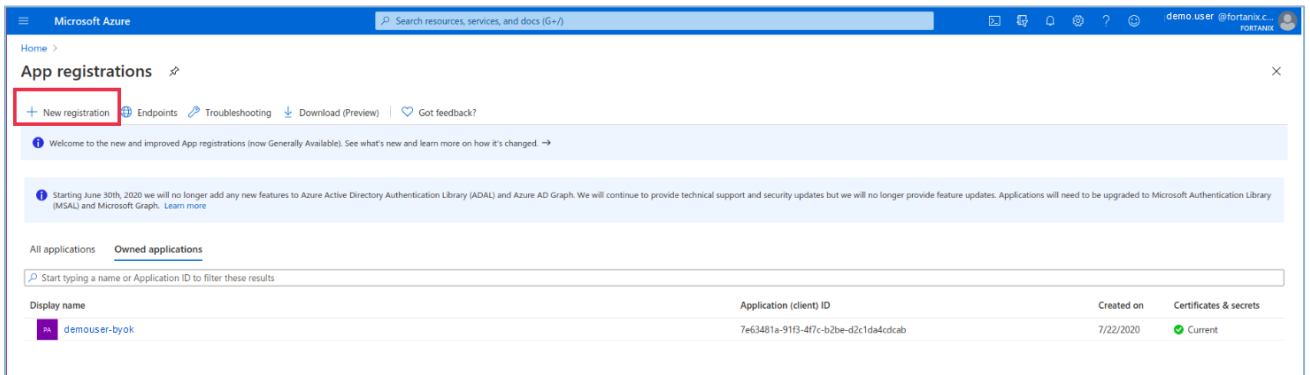


FIGURE 1: INITIATE APP REGISTRATION

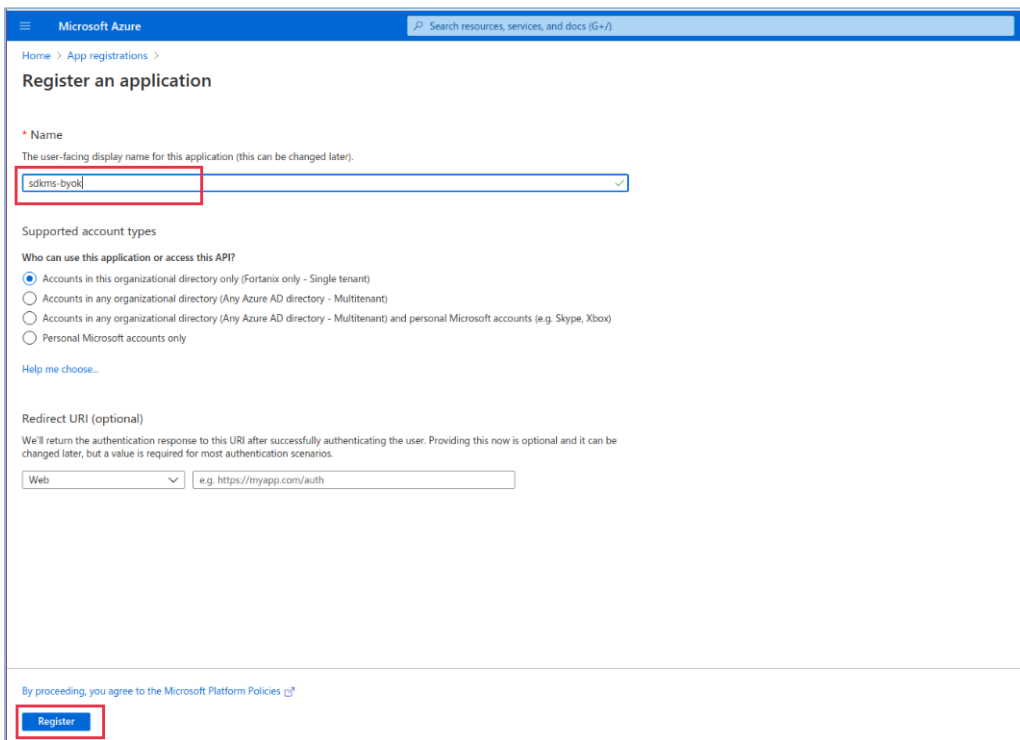


FIGURE 2: REGISTER AN APP

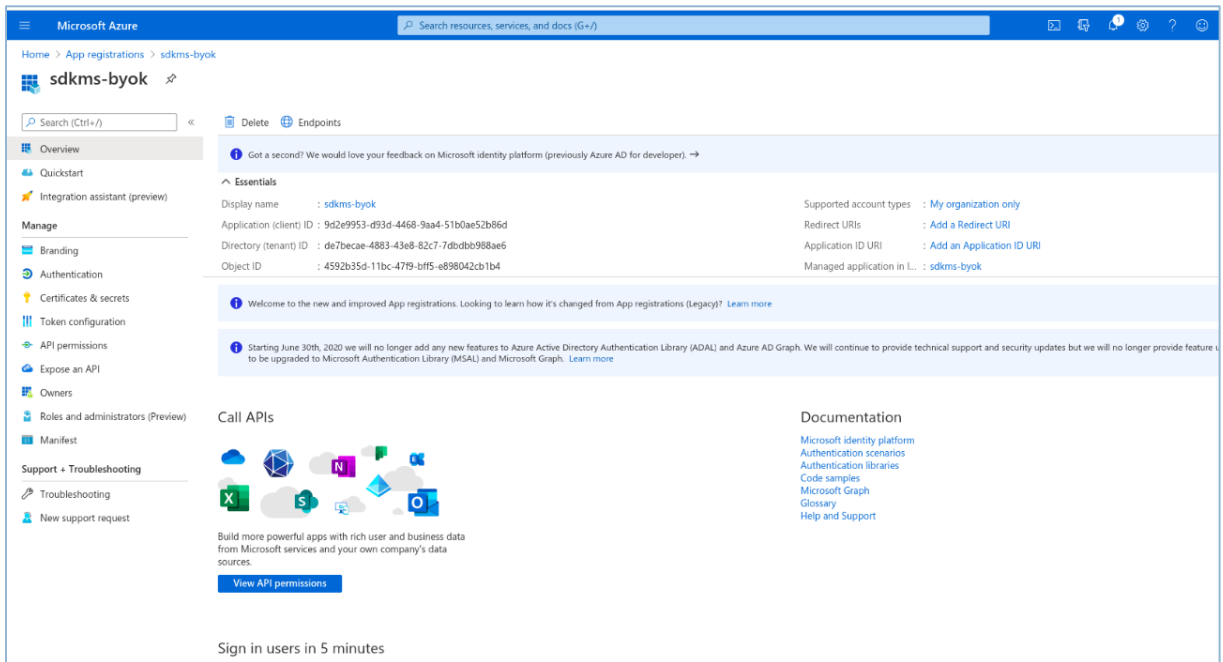


FIGURE 3: APP REGISTERED

3. Upload a client certificate for the above application.

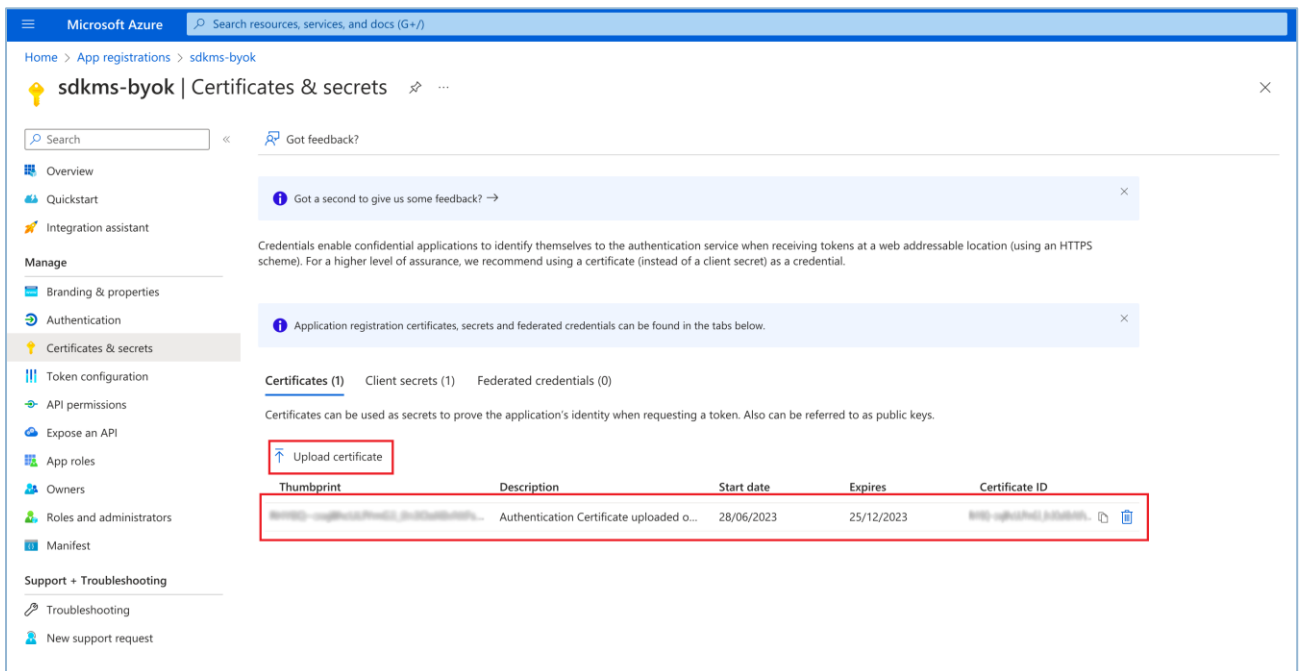


FIGURE 4: CLIENT CERTIFICATE FOR THE APP

Create a client secret for the above application.

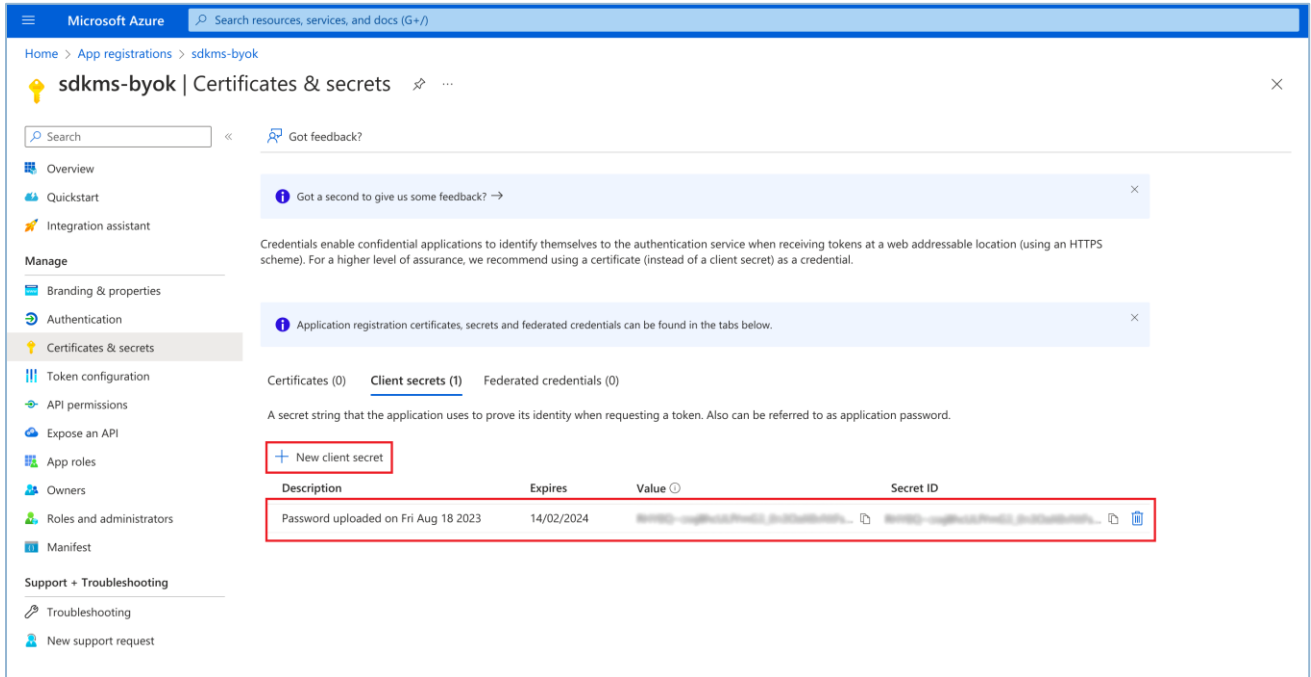


FIGURE 5: CLIENT SECRET FOR THE APP

4. Give the App permission to access the Azure Key Vault.

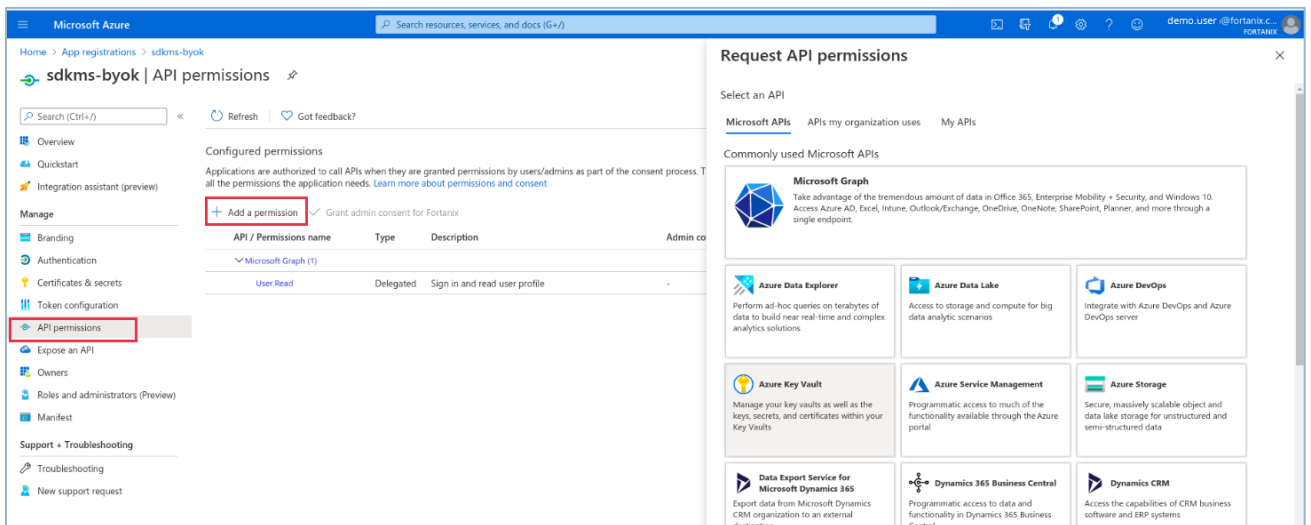


FIGURE 6: KEY VAULT PERMISSION TO ACCESS THE APP

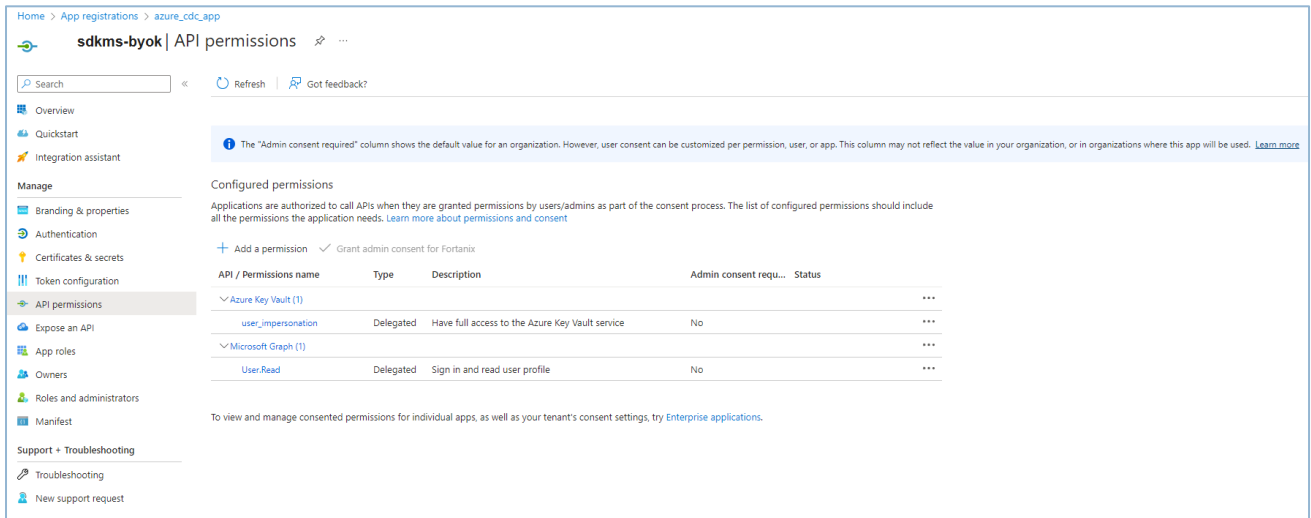


FIGURE 7: KEY VAULT PERMISSION TO ACCESS APP

5. Create an Azure Key Vault.

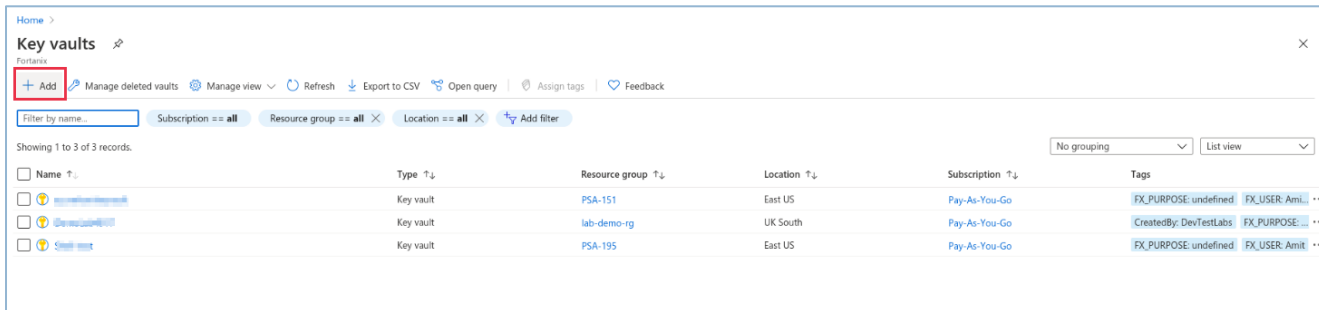


FIGURE 8: CREATE AZURE KEY VAULT

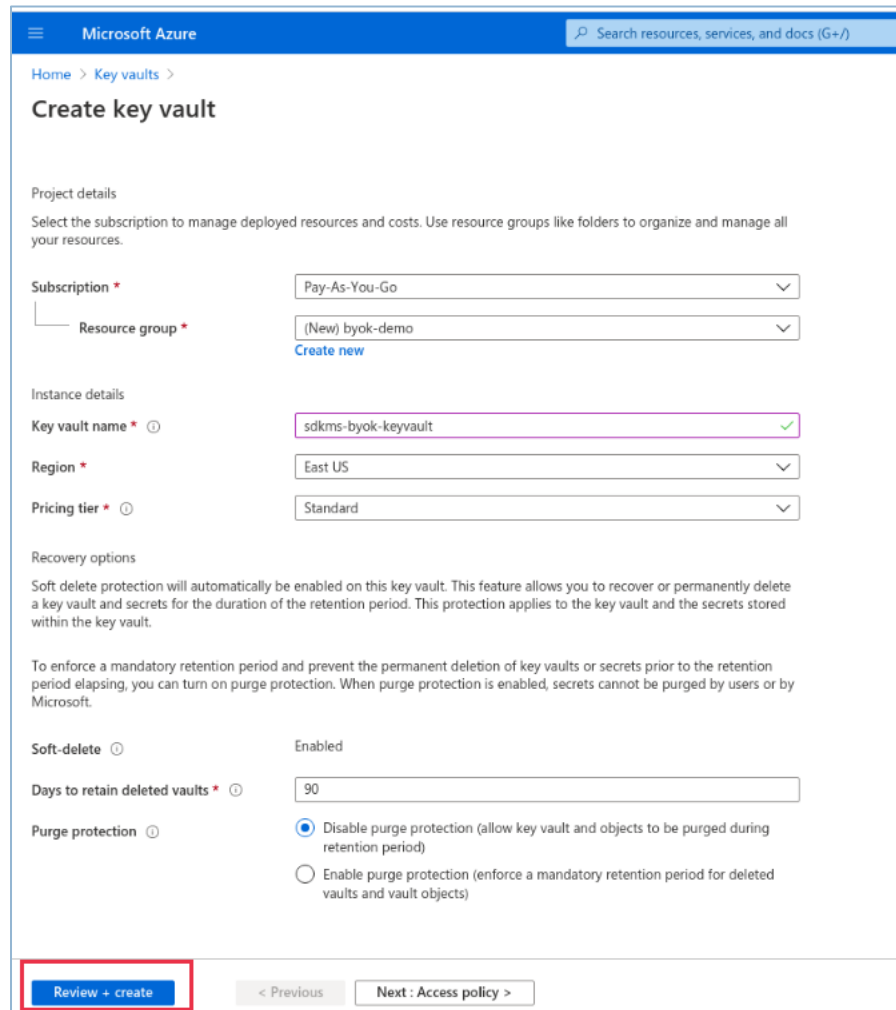


FIGURE 9: CREATE AZURE KEY VAULT

6. Add the application to the Access Policy of the Key Vault.

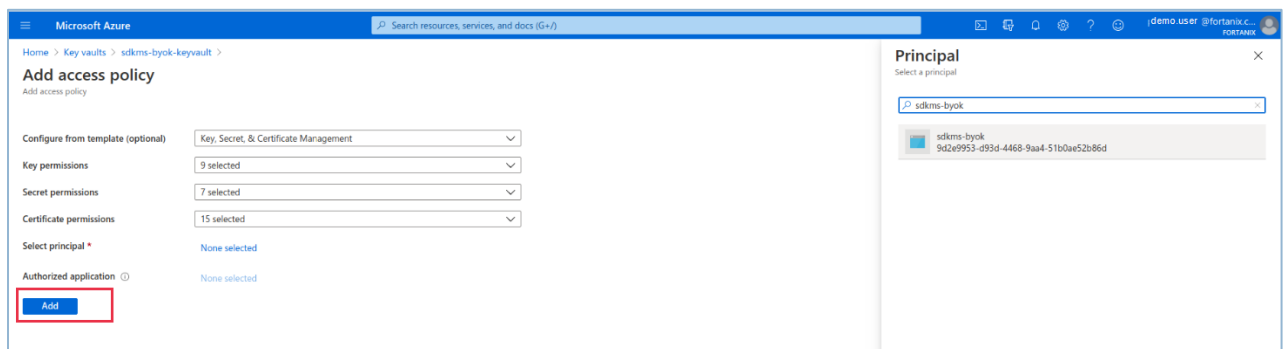


FIGURE 10: ADD ACCESS POLICY

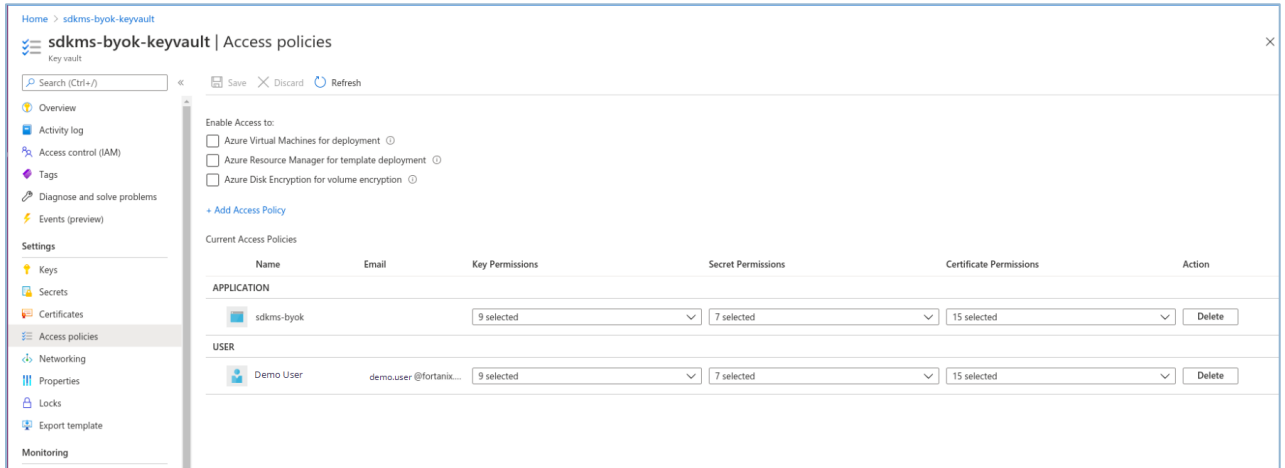


FIGURE 11: ACCESS POLICY ADDED

3.2 CREATE AND CONFIGURE AZURE KEY VAULTS

- Create one or two non-HSM Key Vaults and give 9 key management permissions as explained in **Figures 10** and **11** above.
- Create one or two HSM-backed Key Vaults and give 9 key management permissions as explained in **Figures 10** and **11** above.

3.3 PREREQUISITES

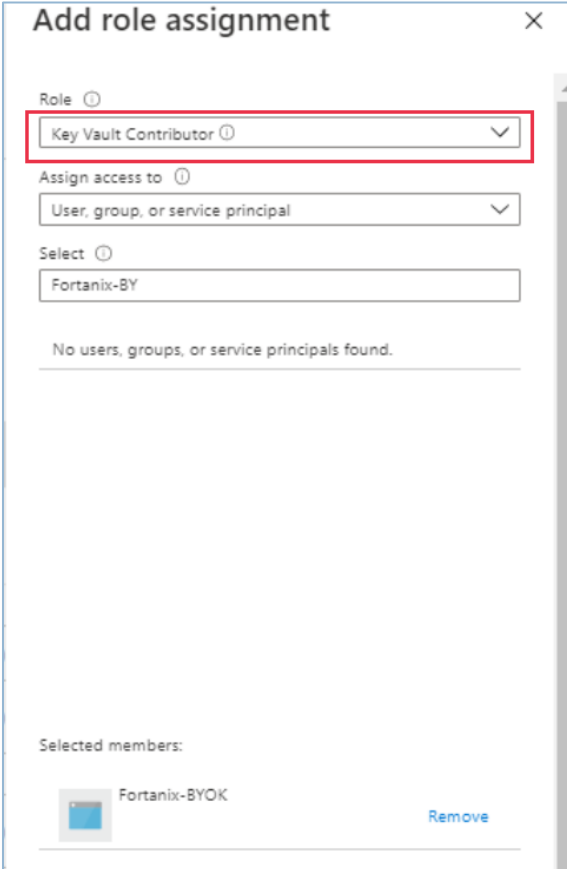
To configure the AKV Managed HSM Fortanix DSM group, the following are the prerequisites that the app in Azure Cloud Data Control (CDC) must have to authenticate the Fortanix DSM group with Azure Key Management Services.

- The app’s API permissions to access the Key Vault. Refer to *Refer to **Figures 6 and 7** above for more details.*
- Adding the app to the Access Policy of the Key Vault. *Refer to **Figure 10** above for more details.*



NOTE: The access policies for the app registered to the key vault should include the permissions: "GET", "LIST", "UPDATE", "CREATE", "IMPORT", "DELETE", "RECOVER", "BACKUP", "RESTORE", "PURGE".

- Register the app as a key-vault contributor in role assignment.
 - In the Azure portal, open your Key Vault.
 - Click **Access Control (IAM) -> Add -> Add role assignment.**
 - In the Add role assignment panel, select the **Role** as **Key Vault Contributor.**



Add role assignment [X]

Role ⓘ
Key Vault Contributor ⓘ

Assign access to ⓘ
User, group, or service principal

Select ⓘ
Fortanix-BY



No users, groups, or service principals found.

Selected members:

Fortanix-BYOK [Remove]

FIGURE 12: ADD ROLE ASSIGNMENT

3.4 CONFIGURE THE AZURE MANAGED HSM

1. On the Fortanix DSM **Groups**  page, click the  button to create a new Azure Managed HSM group.
2. In the **Add new group** form,
 - a. Enter a title and description for your group.
 - b. Next, click the **LINK HSM/EXTERNAL KMS** button to choose the Azure Managed HSM type, so that Fortanix DSM can connect to it.

3.4.1 CREATE AZURE KMS GROUP

1. Select the type of HSM/external KMS as **Azure Managed HSM** in the drop down.
 2. In the **Choose Service** field, select from the following Azure services that you want to authenticate against and establish a successful Azure Managed HSM connection
-

You can choose from the following Azure services:

- **global Azure**
- **Azure for US Government**

Select the “**global Azure**” option to authenticate and upload the key material to any non-GovCloud Azure service or select the “**Azure for US Government**” option to authenticate and upload key material to the specific Azure service set aside for the US government.



NOTE: To use **Azure US Government**, you need to be a US citizen associated with the US Federal Government or a US government contractor. Please refer to the Cloud Providers' documentation about access to these environments.

3. Use the AD credentials created in Section 3.1 to set up an Azure-backed Fortanix DSM Group. Azure subscriptions have a trust relationship with Azure Active Directory (Azure AD).

In the **Authentication** section, enter the Azure KMS account credentials:

- **Tenant ID:** Each subscription has a Directory ID/Tenant ID. Enter the Tenant ID.
- **Client ID:** Each subscription has an Application ID/Client ID. Enter the Client ID.
- **Client Secret:** A secret string that a registered application in Azure uses to prove its identity when requesting a token at a web-addressable location (using an HTTPS scheme). Client Secret is also referred to as application password. Enter the “Value” of the Client Secret from the “Client secrets” section in Azure.





NOTE: Currently, Fortanix DSM supports only "Client Secret" value based authentication.

- **Subscription ID:** The Subscription ID is the ID of your Azure AD subscription contains the Key Vaults associated with that Subscription ID. You can get the subscription ID by navigating to **Subscriptions** in the Azure portal. *Refer to [Azure Subscriptions and Roles](#) for more details.*

Refer to **Figure 3** and **Figure 4** in [Fortanix DSM with Azure Use Case Guide](#) to get the Tenant ID, Client ID, and Client Secret.

3.5 TEST CONNECTION

1. Click **TEST CONNECTION** to test your Azure KMS connection. If Fortanix DSM is able to connect to Azure using your connection details, then it shows the status as “Connected” with a green tick  and fetches the key vaults associated with the Subscription ID. Otherwise, it shows the status as “**Not Connected**” with a yellow warning sign .

3.6 SELECT AZURE MANAGED HSM INSTANCE

Azure Key Vault provides two types of resources to store and manage cryptographic keys: Vaults and Managed HSMs. Vaults support software-protected and HSM-protected keys. Managed HSMs only support HSM-protected keys.

For more details about the types of resources that Azure key vault provides, refer to [Azure documentation](#).

When the Azure KMS is connected successfully, it will enable the **Managed HSM Instance** field. From the list of Managed HSM instances for the Subscription ID entered, select an HSM instance. Click **SAVE** to save the group.

3.7 ADD CERTIFICATE



NOTE: If you are using a configuration such as a proxy for the Azure Managed HSM connection, use this section to add certificates so that Fortanix DSM would allow the use of a custom certificate.

1. Click **+ ADD CONFIGURATION** to add a certificate for authenticating your Azure Managed HSM. There are two certificate options to choose from.
 - **Global Root CA** - Use this certificate if you are using a certificate that is signed by a well-known public CA. By default, every Azure Managed HSM group is configured with a Global Root CA Certificate.
 - **Custom CA Certificate** - Use this certificate if you as an enterprise want to self-sign the certificate using your own internal CA. You can override the default Global CA cert with a Custom CA Certificate for an Azure Managed HSM group. You can either upload the certificate file or copy the contents of the certificate in the textbox provided.

- Client Certificate (optional): A Custom CA Certificate also has a Client Certificate section where you can configure a client certificate and a private key (Fortanix DSM Certificate and Key). This allows Fortanix DSM to authenticate itself to the AKV Managed HSM and vice versa.
- Select the **Validate Host** check box to check if the certificate that the Azure Key Vault provided has the same `subjectAltName` or `Common Name (CN)` as the hostname that the server certificate is coming from.

3.8 THE HSM/KMS TAB

After you save your group details, your group is created, and you will see a detailed view of your group. Now you can see that there is an addition of the **HSM/KMS** tab in the group details, this tab shows the details about your KMS.

The **HSM/KMS** tab shows the details of the KMS that was added such as the Tenant ID, Client ID, Client Secret, Subscription ID, and Managed HSM Instance.



NOTE: You can only edit the Tenant ID, Client ID, and Client Secret to update the Azure KMS connection details. The Azure Managed HSM Instance is non-editable.

Once you edit the connection details and save it, click **TEST CONNECTION** to test the connection. Click **SYNC KEYS** to sync keys from the configured Azure Managed HSM to the Azure-backed Managed HSM Fortanix DSM group.

3.9 SYNC KEYS

When you edit the Azure Key Vault connection details in the Azure Managed HSM group detailed view under **HSM/KMS** tab, click **SYNC KEYS** to import new keys. On clicking **SYNC KEYS**, Fortanix DSM connects to Azure Managed HSM and gets all the keys available. Fortanix DSM then stores them as virtual keys.




NOTE:


- When keys are synced with Azure Managed HSM, an encrypted backup of the newly discovered keys from the Azure Managed HSM is escrowed into Fortanix DSM. In the event of a key purged from the Azure Managed HSM, this escrow can be used to restore the key. The actual key material for those keys is always stored in Azure Managed HSM.

- Clicking **SYNC KEYS** only returns the keys from Azure Managed HSM that are not present in Fortanix DSM. That is, every click will append only new keys to Fortanix DSM.
- The time taken to sync keys from Azure Managed HSM to Fortanix DSM is a function of the number of keys in the Azure Managed HSM and the network latency between Azure location and DSM. It can take several minutes if there are hundreds of keys and there is significant network latency.


3.10 NOT CONNECTED SCENARIO

On clicking **TEST CONNECTION**, it is possible that Fortanix DSM is not able to connect to the Azure Managed HSM, in that case, it displays a “**Not Connected**” status with a warning symbol . You can save the details of the new connection details provided and edit them later.

3.11 GROUPS TABLE VIEW

After saving the group details, you can see the list of all groups and notice the special symbol  next to the newly created group, this symbol differentiates it from the other groups, as it shows that it is an external KMS group.

3.12 USER VIEW

Click the **Users** tab  in the Fortanix DSM UI and click the user that says “**You**” to go to the user’s detailed view, as shown below.

The detailed view shows all the groups which the user is a part of, additionally Fortanix DSM displays which groups are mapped to Azure Managed HSM and whether they are “Connected” or “Not Connected”.



4.0 FORTANIX DATA SECURITY MANAGER AZURE MANAGED HSM SECURITY OBJECTS


4.1 CREATE A KEY IN AZURE MANAGED HSM GROUP – GENERATE (MANAGED HSM POOL)

You can generate a key in a configured Azure Managed HSM (Managed HSM Pool).

4.1.1 GENERATE A KEY

This action will generate the configured key type in the Azure Managed HSM Pool, and it will be represented as a virtual key in the corresponding Azure Managed HSM group. This means that the virtual key in the Azure Managed HSM group will point to the actual key in the Azure Managed HSM Pool that stores the key material of this new key. The virtual key only stores the key information and key attributes, but it does not have the key material. In your Fortanix DSM console, follow the process below to create a new key:

1. Click the **Security Objects**  tab.
2. Click  to create a new Security Object.
3. In the **Add New Security Object** form, enter a name for the Security Object (Key).
4. Select the **This is an HSM/external KMS object** check box. This will show the Azure Managed HSM configured groups in the **Select group** list.
5. In the Azure group list, select the Azure Managed HSM group into which the keys will be generated. The **Azure Managed HSM** Instance associated with the Azure group is displayed.
6. Select **GENERATE IN AZURE** to initiate the generate key in Azure workflow.
7. Enter the **Azure key name**: The Azure key name is the key name that will be stored in Azure Key Vault. The Azure key name will be used to correlate between different versions of a key. All the key versions will have the same Azure key name.
8. Select the key type for the new Azure KMS key.

 **NOTE:** The allowed key types for an Azure Managed HSM key generated using the Generate Key workflow are:

- RSA key pairs (RSA_2048, RSA_3072, and RSA_4096)
- AES 256



These key types can further be restricted by setting a crypto policy for the account or group. *For more details about the crypto policy, refer to the article:*

<https://support.fortanix.com/hc/en-us/articles/360042064051-User-s-Guide-Crypto-Policy>.

The key types can also be restricted by setting a Key metadata policy for the group. *For more details about the Key metadata policy, refer to the article:*

<https://support.fortanix.com/hc/en-us/articles/4420883272596-User-s-Guide-Key-Metadata-Policy>

<https://support.fortanix.com/hc/en-us/articles/360042064051-User-s-Guide-Crypto-Policy>.

9. Enter the **Key size**.
10. Enter the key **Activation Date**, and key **Deactivation Date**.
11. Select the permitted key operations under **Key operations permitted** section.
12. Add any key tags if required using **ADD TAG**.
13. Click the **GENERATE** button to generate the key in Azure Managed HSM.
14. The new Azure Key is created and represented with a special symbol  to denote it is of type "External KMS". In the detailed view of the Azure key, you will notice the following things:
 - The "key state" - whether the key is in a pre-active/active state based on the "activation date" selected during the key creation.
 - The Azure Key Name appears on the top.
 - The group to which it belongs (in the **Group** field). It also shows if the group is mapped to Azure Managed HSM or not using the special icon .
 - How the key was created (in the **Created by** field). If it is an Azure Managed HSM key, this field shows the group that created this key. It also shows minor details such as if the group is "Connected" or "Not Connected".
15. The new key will be added to the Security Objects table.



Tip:

- You can also access the new key from the Group detailed view from the **SECURITY OBJECTS** tab.
- You can also add a new key from the Group detailed view from the **SECURITY OBJECTS** tab, click **ADD SECURITY OBJECT**, and follow **steps 3-13** above.

Go to the **AZURE KEY DETAILS** tab to see the properties of the Azure Key such as the Version Number and Resource ID of the key.

Log in to the Azure console and verify if the new key is generated successfully.



NOTE: When a new key is created in the Azure Managed HSM from Fortanix DSM, a backup blob for the key (along with its key versions) will be downloaded from Azure and saved into Fortanix DSM when a **SYNC** is performed on the group.

4.1.2 BRING YOUR OWN KEY – IMPORT KEY

This action will import the configured key type in the Azure Managed HSM Pool directly, and it will be represented as a virtual key in the corresponding Azure Managed HSM group. This means that the virtual key in the Azure Managed HSM group will point to the actual key in the Azure Managed HSM that stores the key material of this new key. The virtual key only stores the key information and key attributes, but it does not have the key material. The import action will not store a copy of the key material in Fortanix DSM.

1. Follow Steps 1-5 from *Section 4.1.1*
2. Select **IMPORT** to initiate the import key in Azure workflow.
3. Enter the **Azure key name**.
4. Select the key type for the new Azure KMS key.



NOTE: The allowed key types for an Azure key generated using the import key workflow are:

- RSA key pairs (RSA_2048, RSA_3072, and RSA_4096)
 - AES 256
5. Sometimes keys of type RSA that need to be imported from a file were previously wrapped (encrypted) by a key from Fortanix DSM. This is done so that the key should not go over the TLS in plain text format. In such scenarios select the check box **The key has been encrypted**.
 - a. Next enter or select a Key ID or SO name in the **Select Key Encryption Key** section which will be used to unwrap (decrypt) the encrypted key in the file which will later be stored securely in Fortanix DSM. This key should have already been created or imported in Fortanix DSM.
 6. Click **UPLOAD A FILE** to upload the key file in **Raw**, **Base64**, or **Hex** format.

7. Enter the key **Activation Date**, and key **Deactivation Date**.
8. Select the permitted key operations and any key tags if required using **ADD TAG**.
9. Click **IMPORT** to import the key.
10. The key is successfully imported.



NOTE: When a new key is created in the Azure Managed HSM Pool from Fortanix DSM, a backup blob for the key (along with its key versions) will be downloaded from Azure and saved into Fortanix DSM when a **SYNC** is performed on the group.


4.1.3 BRING YOUR OWN KEY – COPY KEY TO AZURE KEY VAULT

Use this option when you want to generate a key in Fortanix DSM and then import the key into the configured Azure Managed HSM. The copy key to the Azure feature will copy a security object from one regular Fortanix DSM group to another regular/Azure Managed HSM Fortanix DSM group. This feature has the following advantages:


- Maintains a single source of key material while using/importing that key into various Fortanix DSM groups where applications may need to use a single key to meet business objectives.
- Maintains a link of various copies of the same key material to the source key for audit and tracking purposes.

The following actions will happen as part of the copy key operation:


- A new key will be created in the target group: The new key will have the same key material as the original.
- The source key links to the copied keys: There will be a link maintained from all copied keys to the source key.
- The Source key will also have basic metadata-based information about the linked keys such as:
 - Copied by <user-name/app id>
 - Date of Copy <time stamp>
 - Target copy group name

 **NOTE:** The name of the copied key is suggested automatically to the user as [original key name]_[copy1,2,...], but can be replaced with an alternative unique name.

To copy a key from a regular Fortanix DSM group to an Azure Managed HSM group:

1. Go to the detailed view to a key and click the **NEW OBJECT** icon  on the far right of the screen.
2. In the menu that appears, click the **COPY KEY** button.

 **NOTE:**

- The allowed key types for an Azure Managed HSM key generated using the copy key workflow are:
 - RSA key pairs (RSA_2048, RSA_3072, and RSA_4096).
 - AES 256
 - The RSA and EC key to be copied must have the “Export” permission enabled or the copy key operation will fail.
 - The **COPY KEY** button will be disabled for all the Azure Managed HSM virtual keys.
3. In the **COPY KEY** window, update the name of the key if required using the edit  icon.
 4. Click the **Import key to HSM/External KMS** check box to filter the groups to show only HSM/AWS KMS/Azure KMS groups. Select the Azure Managed HSM group for the new key into which the copied key should be imported.
 5. Enter the **Azure key name**.
 6. Update the **KEY PERMISSIONS** if you want to modify the permissions of the key.
 7. Click **CREATE COPY** to create a copy of the key.
 8. The source key will now appear as a key link in the **KEY LINKS** tab in the detailed view of the copied key.

 **NOTE:**

- If a user wants to maintain a copy of the key material in Fortanix DSM, then the user can import a regular RSA/AES key into Fortanix DSM using the “import key” workflow and then copy this key into Azure Managed HSM using the “copy key” workflow.

4.2 ATTRIBUTES/TAGS TAB

This tab will have all the tags of the Azure Managed HSM key. You can add new tags using the **NEW TAG** button.


4.3 AZURE KEY DETAILS

This tab displays details of the Azure key properties such as Resource ID and Key version number. The **AZURE KEY DETAILS** tab also contains **SOFT DELETE KEY** option, which is explained in *Section 4.6*.

4.4 SECURITY OBJECTS TABLE VIEW

After you add new Azure keys, go to the **Security Objects** page to view all the security objects from all the groups (Regular and HSM/External KMS).

In the security object table, you will notice that every key belongs to a group and some keys which are virtual keys added from an Azure Managed HSM, belongs to a group with a special symbol

 . The security objects table view will continue to show all the keys irrespective of if they belong to an Azure Managed HSM group or not.

4.5 DEACTIVATE A KEY IN AZURE GROUP

When you deactivate an Azure key in Fortanix DSM, the action will deactivate the virtual key in Fortanix DSM and the actual key in the configured Azure Managed HSM will be disabled.

To deactivate a key:

1. Select the Azure key to deactivate.
2. In the security object detailed view, scroll down, and click the **DEACTIVATE** button.

4.6 SOFT DELETE A KEY IN AZURE MANAGED HSM

Soft delete deletes a key from an Azure Managed HSM which was already scanned in the Azure Managed HSM group in Fortanix DSM with a link to recover this key. Now, when you click **SYNC KEYS** in Fortanix DSM:

- The status of the key in the Azure KMS group will become “soft-deleted in Azure”.

- The key can only be recovered for a retention period set in the key vault.
- If you choose to recover this key, the virtual key will become active as well as the actual key will become active in the Azure Managed HSM.
- If you do not recover the key within the retention period, the Azure Managed HSM will automatically purge and delete the key permanently.

To delete a key from Azure Managed HSM:

1. Go to the detailed view of an Azure virtual key and select the **AZURE KEY DETAILS** tab.
2. Click the link **SOFT DELETE KEY**.
3. In the Soft Key Deletion in Azure Managed HSM window, select the confirmation **“I understand that the key is not usable for Sign/Verify, Wrap/Unwrap or Encrypt/Decrypt operations once it is deleted.”**
4. Click **SOFT DELETE KEY** button to mark the key for deletion.
5. You can recover the deleted key any time before the retention period ends using the **RECOVER DELETED KEY** link on the top of the screen in the detailed view of the virtual key. When the “Recover Key” link is clicked, the key will be recovered back in Azure Managed HSM with all its versions.

**NOTE:**

- When the retention period ends, the key gets purged and deleted permanently. However, even if the key is purged in Azure Managed HSM, if the key was imported from Fortanix DSM, then the same key material can be re-imported into Azure Managed HSM from the backup blob.
- In the Azure Managed HSM, when a key is deleted, all its versions get deleted along with it and when restored, all its versions are restored together.

4.7 DELETE A KEY IN AZURE GROUP

The **DELETE KEY** button will be enabled when the key material has been purged in Azure Managed HSM. When you click **DELETE KEY**, Fortanix DSM will remove the key backup blob, and hence the key cannot be restored.

To delete a virtual key:

1. Select the Azure Managed HSM key to delete.
2. In the security object detailed view, scroll down and click the **DELETE KEY** button.

5.0 ROTATE A KEY IN AZURE GROUP

5.1 ROTATING AZURE NATIVE KEY* WITH ANOTHER NATIVE KEY

**Native key is one where the key material was generated by Azure Managed HSM.*

When you rotate a virtual key in an Azure Managed HSM group, the action will rotate the key inside the Azure Managed HSM by generating another new version of the key within the configured Azure Managed HSM in a nested way by moving the key alias from the old key to the new key.

To rotate a key in Azure Managed HSM:

1. Select the Azure virtual key to rotate.
2. In the detailed view of the Azure virtual key, click the **ROTATE KEY** button.
3. In the Key Rotation window, click the **ROTATE KEY** button to rotate the virtual key.

A new rotated key is now generated.

5.2 ROTATING KEYS IN FORTANIX DATA SECURITY MANAGER SOURCE GROUP

When a key is rotated that belongs to a Fortanix DSM source group and has linked keys that are copies of the Fortanix DSM source key with the same key material as the source key, then the user is given the option to select the linked keys for key rotation. If these linked keys belong to an Azure Managed HSM group, then rotating the linked keys results in rotating the keys in Azure Managed HSM as well by generating new versions of the keys within the configured Azure Managed HSM in a nested manner.

1. Click **ROTATE KEY** in the detailed view of a Fortanix DSM Source Key.
2. In the KEY ROTATION window, select the **Rotate linked keys** check box.
3. Select the Azure Managed HSM virtual keys that need to be rotated along with the Fortanix DSM source key and click **ROTATE KEY** to rotate the linked key.
4. Once the keys are rotated, click the **OK** button.

You can also schedule a key rotation policy for the Fortanix DSM source key such that the linked Azure keys that are copies of the source keys are also periodically rotated automatically.

To schedule a key rotation policy for the source key:

1. Go to the detailed view of the source key in the Fortanix DSM UI.
2. In the detailed view, click the **KEY ROTATION** tab and click the **ADD POLICY** button.
3. Enter the key rotation schedule by specifying the rotation frequency, start date, and time.
4. To deactivate the old key after key rotation, select the **Deactivate original key after the rotation** check box.
5. To rotate the linked copied keys, select the **Rotate all copied keys** check box.
6. Click **SAVE POLICY** to save the policy.

For more information on the key rotation policy, refer to the [User's Guide: Key Lifecycle Management](#).

5.3 ROTATE AZURE NATIVE KEY TO FORTANIX DATA SECURITY MANAGER OWNED KEY

When an Azure Managed HSM virtual key whose key material is owned by Azure Managed HSM is rotated, the user is given an option to rotate the virtual key with a Fortanix DSM-backed key. When the user selects this option and performs the rotation, a new virtual key is created, with the corresponding key in Azure Managed HSM, which has the key material of the Fortanix DSM backed key. As a result, the Azure Managed HSM virtual key is backed by a Fortanix DSM Source key.

To rotate a virtual key with Fortanix DSM backed key:

1. Click **ROTATE KEY** in the detailed view of an Azure virtual key.
2. In the Key Rotation window, select the **Rotate to S-D KMS key** check box.
3. Select the Fortanix DSM group that contains the source key.
4. Select the source key and click the **ROTATE KEY** button.

The Virtual key is successfully rotated and backed by the source key. To confirm go to the detailed view of the newly rotated Azure virtual key and click the **AZURE KEY DETAILS** tab. The **SOURCE** field now points to "FortanixHSM" instead of "External".

6.0 DOCUMENT INFORMATION

6.1 DOCUMENT LOCATION

The latest published version of this document is located at the URL:

<https://support.fortanix.com/hc/en-us/articles/5486109561236-User-s-Guide-Azure-Managed-HSM>

6.2 DOCUMENT UPDATES

This document will typically be updated on a periodic review and update cycle.

For any urgent document updates, please send an email to: support@fortanix.com

6.3 REVISION HISTORY

DOCUMENT VERSION	DATE PUBLISHED	CONTRIBUTORS	PREPARED BY	APPROVED BY	SUMMARY OF CHANGES
1.0	11 APR 2022	KOUSTAV SAHA	N. RAMAKRISHNAN		INITIAL PUBLICATION
1.1	26 APR 2022	DEVANSH BANSAL	N. RAMAKRISHNAN		LINKED KEY ROTATION
2.0	07 JUNE 2023	SANDER TEMME	N. RAMAKRISHNAN		SUPPORT FOR AZURE GOV CLOUD

© 2016 – 2023 Fortanix, Inc. All Rights Reserved.

Fortanix® and the Fortanix logo are registered trademarks or trade names of Fortanix, Inc.

All other trademarks are the property of their respective owners.

NOTICE: This document was produced by Fortanix, Inc. (Fortanix) and contains information which is proprietary and confidential to Fortanix. The document contains information that may be

protected by patents, copyrights, and/or other IP laws. If you are not the intended recipient of this material, please destroy this document and inform info@fortanix.com immediately.